International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Provocations Open Problems Encountered By Digital Forensics Ensuing Trends in Near Future

Malik Basit Ahmad
Student, Department of Computer Science Engineering, School of Engineering Sciences Technology, Jamia Hamdard, New Delhi, India

ABSTRACT
There has been a substantial and extensive use of Internet and technology in present day life which relatively has made the digital devices apropos to criminal investigations or legal prosecutions. Investigating huge amount of digital evidence consisting of data in various formats requires a digital forensic analysis (or cyber forensics). As the number of cases keeps on growing continuously, it is expected that the digital forensic analysis will increase significantly in near future. The forensic process involves the examination of digital devices which include computers, cell phones, devices supporting IoT, network formations like LAN's, WAN's etc. These varieties of digital evidence sources can anticipate new challenges for the investigation teams entrusted for imaging, analysis, storage and prosecution of the corresponding evidences. This paper reviews existing research literature and drafts the challenges from the technical standpoints and also elevates the estimation of future trends that could assist in more effective and robust digital forensic process.

Keywords: *digital evidence; digital forensic analysis (cyber forensics); challenges; future trends*

INTRODUCTION
Digital Forensics is the collection and examination of the evidence residing on electronic devices and consequent reactions to threats and assaults which further involves revealing and deciphering suspected information. The basic idea behind the process is to preserve any evidence in the original form while performing a structured investigation by collecting, identifying, validating and reporting the digital information for the purpose of reconstructing the past Events. In present era, various digital devices such as phones, computers, PDA's, Io T assisted devices etc. and network formations like LAN's, WAN's, MAN's etc. have become of utmost importance. There is a possible bent that the data (or any other information) obtained from these devices or networks can be used for criminal activities such as hacking, cracking, ATM frauds, e-money laundering, cyber terrorism, cyber bullying, unlawful intrusion or any other computer assisted fraud or crime which stand ready to bring organizations to their knees [1] . Computer crimes or cyber crimes can have a notable socioeconomic impact on organizations. Thus, investigations need to be carried out promptly so that the criminals are identified and prosecuted on the nail. Since, the range of data sources is increasing at a rapid pace and hence it requires a multitude of devices for storage. Further, with the emergence and acquisition of more secure technologies such as IOT, cloud computing, big data, encryption (which now covers the full disk encryption), secure network communication, secure processors and anonymous routing potentially make the things more complex. Given these arrays of problems and complexities will henceforth give rise to new provocations and hence may dense the application areas of Cyber Forensics. The developmental work in the field of communication and technology is expected to diversify the field of Cyber Forensics further. The opening sections of this paper describes some of the challenges due to the advancements in technology and the second part describes the future trends which once implemented could assist in prompt digital forensic process.

PROVOCATIONS AND OPEN PROBLEMS:

With the drastic extension and revolution in the field of computer science and network technologies the use of pre-existing tools and techniques used for forensic analysis have become less effective. This revolution has given birth to data from many sources of digital evidences and that too in variety of formats as already described. Analysis of the data and then generating the meaningful results thus becomes the greatest forensic challenge facing law enforcement. Further criminals use anti- forensics to frustrate or create an overhead to forensic tools, investigations and investigators [2]. Some of the major challenges considered to be overhead for Cyber Forensics are described as follows:

Inception of Big Data

Big Data is a talk of today. It is an evolving term that describes voluminous amount of unstructured, semi-structured or structured data that has a potential to be mined for information. The diversity of big data is characterized by Volume, Velocity, Variety, Veracity and Value of the data which sometimes is also referred to as 5 V's of Big Data. Due to its scale, diversity and complexity there is a requirement for designing and developing new architectural framework, techniques and algorithms so as to harness the hidden knowledge from it [3]. Here the prime challenge is to identify and collect the evidence in a timely manner, right when the incident happens. In addition to this bitwise acquisition is not a systematic approach due to the size of evidence item. Again, preservation of an evidence item requires large disk space which calls for a considerable investment in forensic labs. For analysis, there is still exists a skill gap in present era for dealing with huge amount of data. The final report is expected to reveal accurate evaluation of tools, methods used and results generated. Although, certain tools like Map Reduce, Natural Language Processing, Machine Learning, Artificial Neural Networks (ANN) are already in use but they are not suitable for forensic work and hence new procedures and methods need to be developed leveraging Big Data [4][5].

Boundless Social Networking*:*

Use of social networking has gained a momentum from the past few years and the numbers of users of these services are increasing at a rapid pace. For example, Face book currently claims to have 950 million users connected across the globe and same is the case with other social networking platforms like Twitter, WhatsApp, Vibe, Snap chat, Instagram etc. which ultimately has provided feasibility to connect anywhere, anytime on any device in everyone's hand. The increasing use of social media has facilitated the development of some serious cyber crimes and other untoward activities. The persons associated with such activities constantly change their plans and strategies which in turn tend to pose a challenge to forensic investigators [6]. In addition to this the number of users is increasing at a rapid pace, which leads to the exponential data transactions. Visualizing and investigating huge amount of data is another confronting task.

Although, certain tools and other relative programs have been developed which provide online user information, but still the forensic extraction from social networking sites is still has serious research problem in terms of data completeness and data compatibility [7].

Internet of Things (Io T)

In present domain, everything seems to be connected with Internet. Billions and billions of machines and things which include cars, homes, workplaces, watches, glasses, home appliances and possibly all other physical objects that strike our mind are being connected to Internet thus providing remote access to visualize and collect data [8]. Although, with the advent of Internet-of-Things (Io T) the life has become more comfortable but at the same time it has provided an edge to cyber criminals in terms of security and privacy. The spread of this technology thus poses certain challenges when Io T assisted devices are involved in any criminal activities [9].

One of the prime challenges is the analysis of the data spread across different locations. In Io T, data could be spread across different locations like cloud, third party location, mobile devices etc. Thus, the location of evidence is considered as one of the biggest challenges that can hinder the investigation process [10]. Another challenge is the limited life span of the data mainly due to the limited storage in Io T devices. The life span of the data is short and hence it can be easily overwritten. The major challenge that can resist the forensic investigation is the type of device. As different devices like TV's, refrigerators, smart watches etc. are getting added to Io T library, hence investigating these devices is a challenge in absence of the predefined protocol.

Cloud Computing

With the rapid evolution of cloud computing, there has been a drastic revolution in the field of Information Technology (IT). Certain business establishments and organizations have shifted their route to remote and virtualized environments for deploying their infrastructure which is often hosted and managed by third parties[11][12]. The third party is known as Cloud Service Provider (CSP). The services provided by CSP can be categorized into three divisions: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Cloud computing ultimately involves the data processing and hence data centers and CSP's are always on the hit list of the cyber criminals.

There are certain challenges which once accomplished can lead to major breakthrough in digital forensic investigations. Remote data centres, decentralized data logs, unknown physical locations and volatile data are the prime challenges to investigations [13]. Here investigations are affected because Cloud environment is solely CSP dependent which means that investigator cannot access to virtual instances and meta-data directly. Hence procedures and tools need to be developed to overcome the limitations of forensic investigations to be conducted in cloud environments.

Wield Of Encryption and Anti-Forensics

Use of encryption in devices, wireless networks and anti-forensics are other daunting obstacles that may resist the forensic investigation process. With the motive of improving security, reliability and efficiency new cryptographic algorithms and encryption techniques have been developed which in turn are posing a challenge for forensic investigators for recovering digital evidence from computers or other digital devices [14]. The availability of free encryption tools like True Crypt, Pretty Good Privacy (PGP), Bitlocker, File Vault etc. have provided a wider scope to cyber criminals that can hinder the working process of forensic investigation [15]. With the introduction of encryption into operating systems and Full Disk Encryption (FDE), the investigation has become a challenge. Forensic investigators may encounter full disk encryption interface before machine booting, which therefore makes the recovery of digital evidence a difficult task [14]. The encrypted data or a drive can only be accessed with the help of a key or a password. Investigators traditionally use Brute Force techniques to guess the key or they acquire the image of the drive in order to Decrypt the data or gain access to the drive which often takes a lot of time. While obtaining evidence there is always a slight chance that the drive may be damaged or corrupted. Hence new tools and techniques need to be developed which are robust and can help to gather evidence promptly in a safe manner during forensic investigations.

Anti-Forensics or counter forensics can be defined as the technique which aims to interfere in and hinder the forensic investigation process. It is one of the major upcoming bottlenecks to the forensic investigation. Marc Rogers of Purdue University defines anti-forensics as an attempt to negatively affect the existence, amount and/ or quality evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct [16]. Anti- Forensic tools are designed and developed by the programmers with an aim to hamper the investigation process which can eventually turn out to be the worst nightmare for the investigator. There are no general frameworks developed as of now which could assist in analysis and can gauge the anti-forensic situation. Hence, currently forensic investigations take place in presence of anti-forensic activities which need to be countered.

ENSUING TRENDS:

The bottlenecks and challenges faced by digital forensic investigators have inspired the researchers and the forensic experts to layout the new research fields which need to be worked upon, so that the forensic process is carried out in a prompt manner in near future. Some of the current trending research developments which are under the scanner of forensic experts are explained briefly as follows:

Digital Forensics Compute Cluster (DFORC2) :

Law Enforcement Agencies (LEA's) have been facing investigation backlogs due to the exponential growth of HDD storage space. Use of HDD's with 1 to 2 TB storage space is very common days which further is expected to increase to 10 TB and hence might result in exponential growth of the investigation backlogs. Further, with the inception of Solid State Drives (SSD's) the situation has become even more challenging as they are expected to provide even more storage then spinning disk HDD's.

Hence, investigators need tools which provide quality throughput. To accomplish this objective, Research and Development (RAND) was sponsored by

National Institute of Justice (NIJ) to develop such a tool which could provide distributed computing capability and hence can enhance the pace of the digital forensic process. RAND came up with "Digital Forensics Compute Cluster" (DFORC2) which is designed to provide efficient and cost effective forensic analysis to investigators and LEA's. DFORC2 is an open source project that uses Autopsy, Apache Spark and Kafka. In addition to this it uses other open source software packages that play a vital role in integrating data and file analysis steps so that they can run in parallel rather than in serial process [17]. DFORC2 is designed keeping in mind the reduction in infrastructure cost as it runs on a standalone server or in the Amazon Web Services (AWS). The results when compared with the traditional Autopsy prove to be substantially fast and prompt. In near future RAND plans to establish a high integrity chain of custody for DFORC2.

Digital Forensics as a Service (DFaaS):

With the increase in computing devices and storage such as smart phones, routers, GPS enabled devices, pen drives, flash drives etc. each containing a voluminous data in a timely manner and with limited resources, the investigators are facing certain issues which include backlog, miss of critical time, overlook of relevant data and lack of understanding.

DFaaS which is a cloud based service provides more opportunities to overcome these issues. It is an extension of traditional forensics. Netherland Forensic Institute (NFI) has incorporated DFaaS as a solution to huge volume of backlog cases [18]. It involves the use of shared pool of resources (virtual and configurable) over a computer network to provide services. These resources require least management efforts or human intervention. The inception of this service will have significant implications on forensics in near future. Remarkable efforts have been made by the researchers to develop forensic cloud. Sleuth-Hadoop has made certain efforts to merge forensic tools into cloud but it restricts the investigators to build and design the workflow model for analysis as per the requirements. Hence, the workflow cannot be implemented and constructed dynamically. Besides, certain frameworks have been designed and developed which permit the forensic investigators to define their requirements in XML files, which can be used to select the applications as per requirements and also can be used to generate the corresponding map reduce drivers which plays a vital role in setting up the workflow in cloud environment [19]. Although, potential latency and the available online upload bandwidth can turn out to be the challenges to DFaaS but incorporation of such mechanism can facilitate cloud to cloud based storage event monitoring of virtual systems.

Computer Forensics Field Triage Process Model (CFFTPM):

CFFTP is analogous to the first aid which is conducted just after the incident occurs so as to ease the investigation process during the execution phase. Time being a key factor, this model supports on site analysis of computer systems in question. Prime considerations of this model are:

- Recovery of useable evidence with an immediate effect.
- Identification of victims at acute risk.
- To guide the in action investigation.
- Identification of potential charges.
- To assess the offenders danger to the society in an accurate manner.

Besides this, maintaining integrity of the evidence item for examination and forensic analysis is also the major concern. The ability to perform the examination and analysis on scene in short period of time may assist the investigators to reveal the sensitive leads. This may also help in providing the information which is important from the psychological viewpoint.

The phases of CFFTPM include:

- Planning
- Triage
- Usage/ user profiles
- Chronology/ timeline
- Internet activity
- Case specific evidence

These six phases form upper level of categorization and each phase has pre defined sub phases with a variable task which depends on the specifications of the case, file system and operating system to be investigated.

These six phases constitute a high level of categorization and each phase has several sub-tasks and considerations that vary according to the specifics of the case, file system and operating system under investigation, etc [2]. Further, coupling the field triage processing model with DFaaS can further yield the significant benefits in forensic process.

CONCLUSION

The challenges arising due to the revolution and discovery of new technologies which keep on dropping day in and day out have been creating overhead to forensic experts. In present scenario, digital forensic layout however is not compatible to deal with the huge amount of variable data which changes every instant. With the increase in the number of internet users at an exponential rate, the traditional forensic process is facing complications. Network security, being a trend of today is also hindering the pre-existing forensic process model to some extent. Certain machine learning tools are not validated for forensics as well. These challenges have opened up the new gateways. Hence the field of digital forensics has been diversifying since then. Although, DFORC2, DFaaS and CFFTPM are the current areas of investment for researchers but due to the rapid advancements in the cyber world the efforts need to be amplified in order to match with the present dynamic tech savvy requirements.

REFRENCES

1. Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa, Digital forensics , vol 7 of International Journal of Advanced Research in Computer Science and Software Engineering; pp. 275-276.
2. N. M. Karie and H. S. Venter, Taxonomy of challenges for digital forensics, "Journal of Forensic Sciences", vol. 60, no. 4, July 2015, pp. 885-893.
3. "What Is Big Data and What Does It Have to Do with IT Audit?", ISACA Journal, 2013, pp.23-25.
4. Khan M, Chatwin C, and Young R, "A framework for post-event timeline reconstruction using neural networks" *Digital Investigation 4*, 2007.
5. Pearson G, "A Road Map for Digital Forensic Research". In: *Report from DFRWS 2001, First Digital Forensic Research Workshop, 2001*.
6. Mohd Najwadi Yusoff, Ali Dehghantanha, Ramlan Mahmod, Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS, Elsevier, pp.41-62.
7. S. Teelink and R. Erbacher, Improving the computer forensic analysis process through visualization, Communications of the ACM, vol. 49(2) 2006, pp. 71–75.
8. David Lillis, Brett A. Becker, Tadhg O'Sullivan and Mark Scanlon, Current challenges and future research areas for digital forensic investigation, Annual ADFSL Conference on Digital Forensics Security and Law, May 24, pp. 9-20 .
9. Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT Security: Ongoing challenges and research opportunities. In 2014 IEEE 7th International conference on service-oriented computing and applications pp. 230-234.
10. Liu C., Singhal A., Wijesekera D. , Identifying evidence for cloud forensic analysis. In: Peterson G., Shenoi S. (eds) Advancesin Digital Forensics XIII. 410 of the series IFIP Advances in information and communication technology, In 2017 Springer, Berlin, Heidelberg, pp. 111-130.
11. George Grispos, Tim Storer and William Bradley Glisson, Calm before the storm: The challenges of cloud computing in digital forensics.
12. Stephen O'Shaughnessy, Anthony Keane, impact of cloud computing on digital forensic investigations, HAL, pp. 291-303.
13. Meyer, G., & Stander, A. (2015). Cloud computing: The digital forensics challenge. Proceedings of Informing Science & IT Education Conference (InSITE) 2015, pp.285-299.
14. Eoghan Casey, Gerasimos J. Stellatos, Stroz Friedberg, The impact of full disk encryption on digital forensics.
15. Sarah Lowman, The effect of file and disk encryption on computer forensics.
16. Halim Maulana, Raden Muhammad Khalil Prasetyo, Analyzing the effect of anti-forensics of digital techniques to digital forensics examination.
17. Daniel Gonzales, Zev Winkelman, Trung Tran, Ricardo Sanchez, John Hollywood, and Dulani Woods, Digital Forensics Compute Cluster (DFORC2) – A New High Speed Distributed Computing Capability for Digital Forensics, WMSCI 2017, pp. 126-131.
18. David Lillis, Brett A. Becker, Tadhg O'Sullivan and Mark Scanlon, Current challenges and future research areas for digital forensic investigation, CDFSL Proceedings 2016, pp. 10-20.
19. Yuanfeng Wen, Xiaoxi Man, Khoa Le and Weidong Shi, Forensics-as-a-Service (FaaS): Computer forensic workflow management and processing using cloud , The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013, pp. 208-214.
20. Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota, Computer Forensics Field Triage Process Model, Journal of Digital Forensics, Security and Law.